



FlowViewer

Maintaining NASA's Earth Science Traffic Situational Awareness

Graphic credit: Arizona/New Mexico Fire Imagery, USDA Forest Service; Remote Sensing Application Center; Image acquired from Aqua MODIS; NASA GSFC; June 7, 2011

FlowViewer provides a convenient web-based user interface to Mark Fullmer's flow-tools suite, and now with v4.0, CMU NetSA group's SiLK. The inclusion of the underlying SiLK tool set enables FlowViewer users to continue to use the tool with the newer IPFIX netflow data protocol.

FlowViewer has been developed for NASA's Earth Sciences Data and Information System (ESDIS) networks, and credit goes to NASA for their usual outstanding support of innovation.

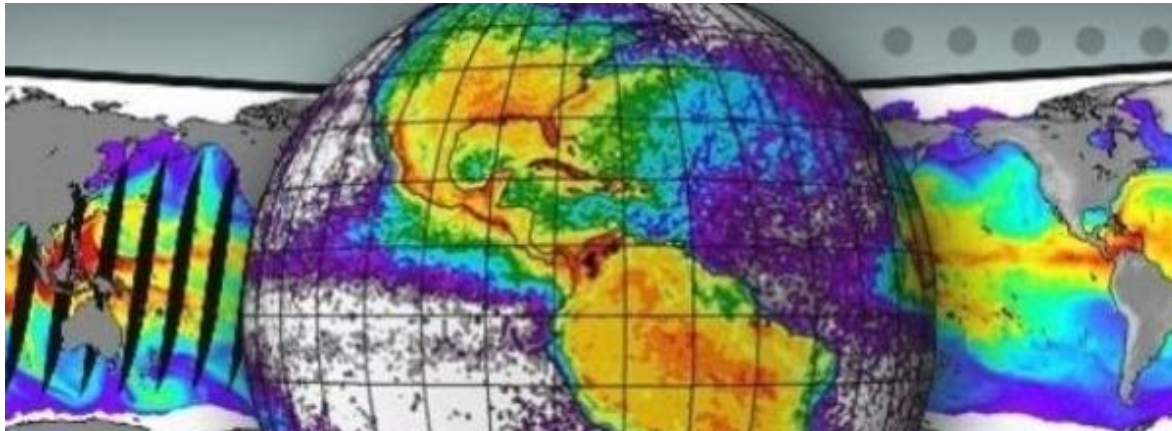


Graphic credit; Hurricane Sandy, October 29, 2012 Captured by Aqua MODIS; EOSDIS Website; NASA official: Kevin Murphy

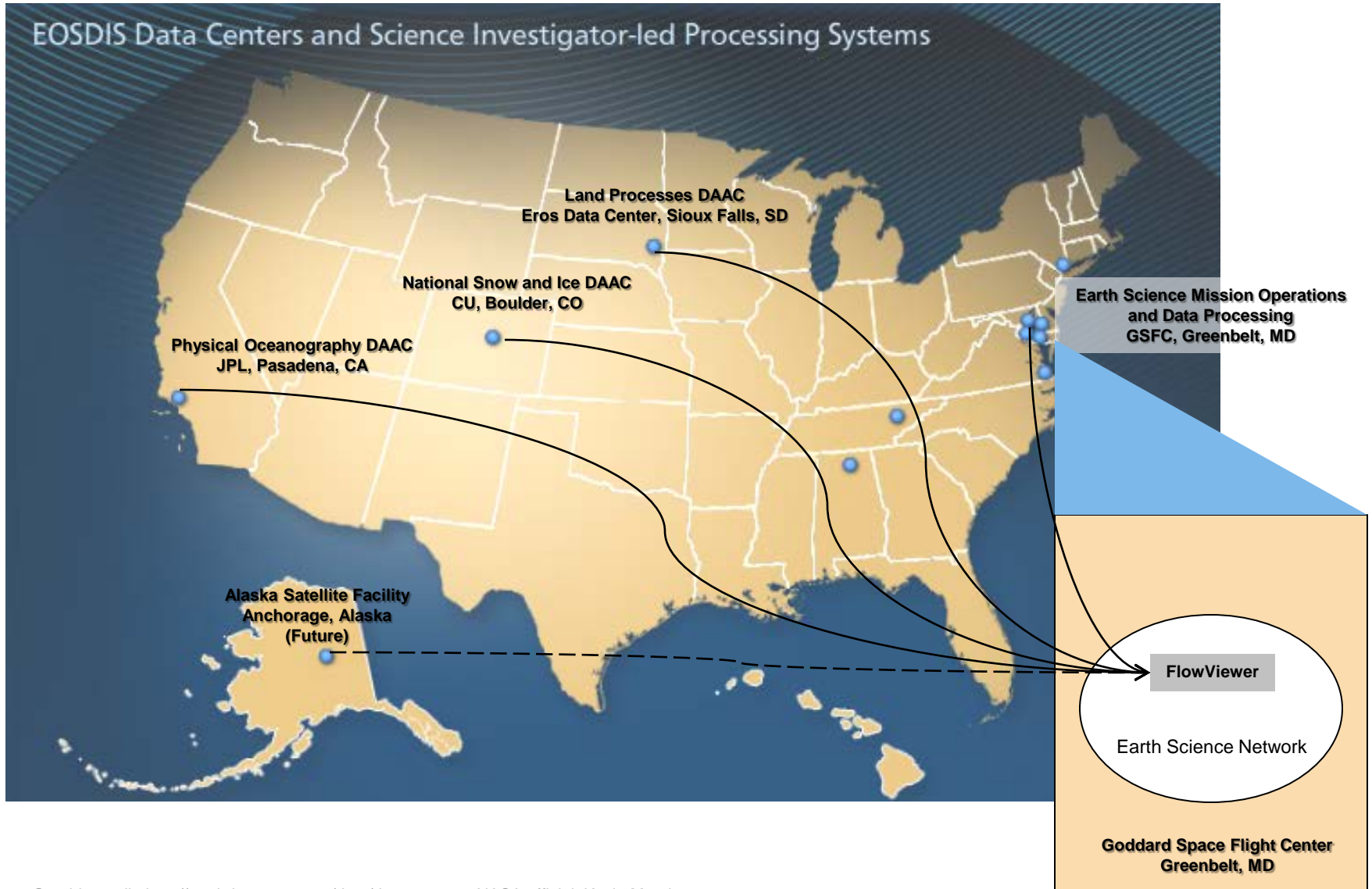


- Complete open-source netflow collector analyzer
- Web-based UI provides dynamic front-end to open source collectors
- Dashboard provides user keep network traffic 'situational awareness'
- Ability to analyze IPFIX netflow (e.g., v9) data captured by SiLK
- Ability to continue to support netflow v5 installations via flow-tools
- Users can graph filtered traffic sets across a specified time period
- Background software tracks filtered traffic over long-term (ala MRTG)
- Ability to save filters and reports for later use and review
- Users can be alerted by email to abnormal data traffic situations

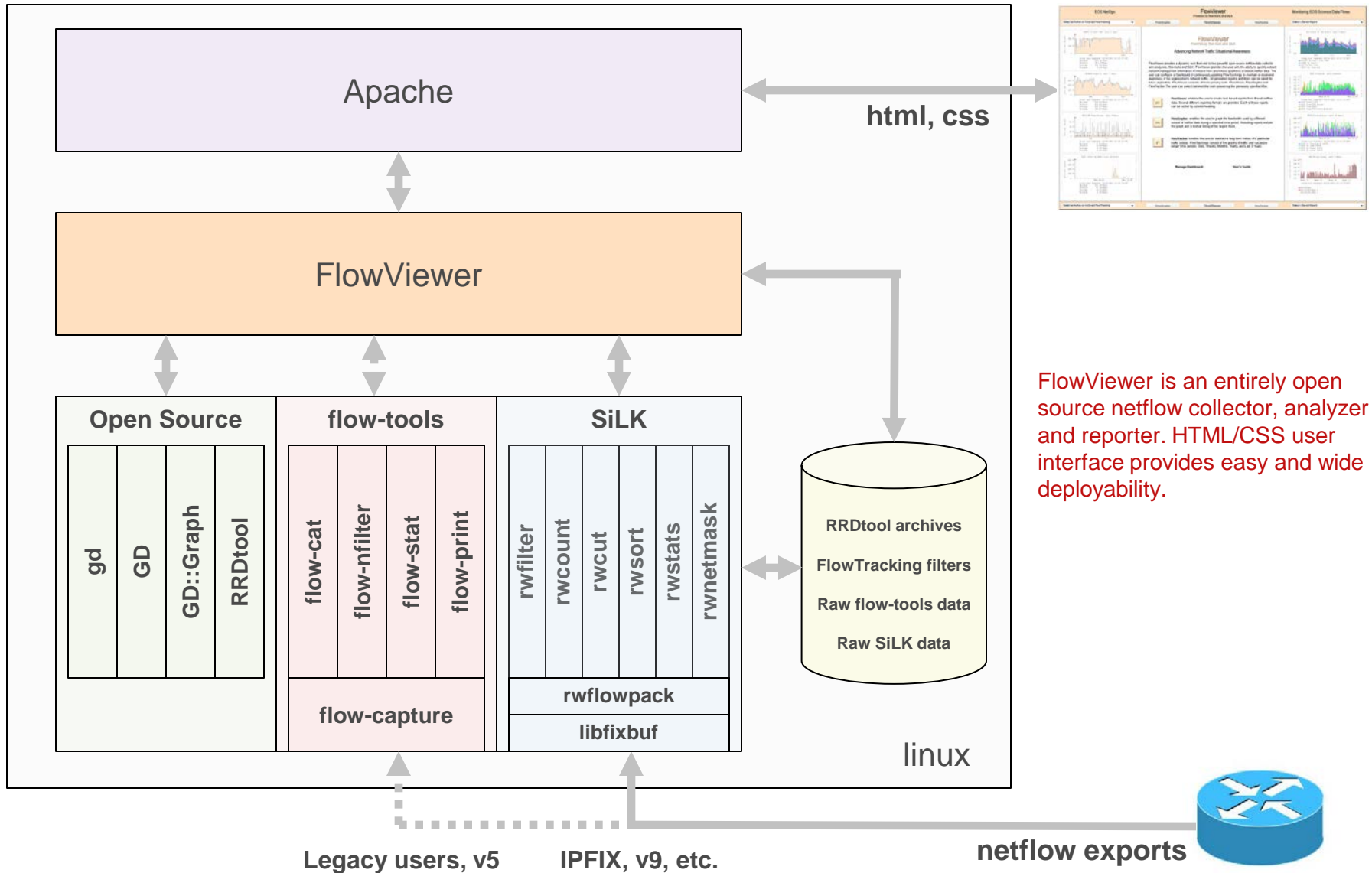
The Earth Observing System Data and Information System (EOSDIS) is a core capability in NASA's Earth Science Data Systems Program. It provides end-to-end capabilities for managing NASA's Earth science data from various sources – satellites, aircraft, field measurements, and various other programs. The EOSDIS serves a broad international community of Earth Science and meteorological scientists and users. Several TBytes of satellite and science data traverse its network every day.



- In 2003 NASA and CSC worked to capture netflow data to help monitor traffic
- Initial capture/analysis system was based on *'cflowd'*
- FlowViewer was developed to aid traffic analysis (away from the command line)
- Today, NASA monitors over 200 Earth Science flows of interest (FlowTrackings)



Graphic credit; <http://earthdata.nasa.gov/data/data-centers> NASA official: Kevin Murphy



FlowViewer is an entirely open source netflow collector, analyzer and reporter. HTML/CSS user interface provides easy and wide deployability.



FlowViewer Main Screen

EOS NetOps

Select an Active or Archived FlowTracking

Graph last updated: 04/30/2012 13:47:27 UTC
 Maximum: 250.20 Rbps
 OS:InAct: 207.33 Rbps
 Average: 258.82 Rbps
 Minimum: 0.88 Rbps

Graph last updated: 04/30/2012 13:47:27 UTC
 Maximum: 684.42 Rbps
 OS:InAct: 636.65 Rbps
 Average: 445.53 Rbps
 Minimum: 304.63 Rbps

Graph last updated: 04/30/2012 13:47:27 UTC
 Maximum: 21.82 Rbps
 OS:InAct: 13.52 Rbps
 Average: 4.30 Rbps
 Minimum: 0.80 Rbps

Graph last updated: 04/30/2012 13:47:27 UTC
 Maximum: 301.26 Rbps
 OS:InAct: 97.28 Rbps
 Average: 14.50 Rbps
 Minimum: 0.80 Rbps

Select an Active or Archived FlowTracking

FlowViewer

Powered by flow-tools and SILK

FlowViewer

Powered by flow-tools and SILK

Advancing Network Traffic Situational Awareness

FlowViewer provides a dynamic web front-end to two powerful open-source netflow data collector and analyzers, flow-tools and SILK. FlowViewer provides the user with the ability to quickly extract network management information of interest from voluminous quantities of stored netflow data. The user can configure a Dashboard of continuously updating FlowTrackings to maintain a situational awareness of his organization's network traffic. All generated reports and filters can be saved for future application. FlowViewer consists of three primary tools: FlowViewer, FlowGrapher and FlowTracker. The user can switch between the tools preserving the previously specified filter.

FV

FlowViewer enables the user to create text based reports from filtered netflow data. Several different reporting formats are provided. Each of these reports can be sorted by column heading.

FG

FlowGrapher enables the user to graph the bandwidth used by a filtered subset of netflow data during a specified time period. Resulting reports include the graph and a textual listing of the largest flows.

FT

FlowTracker enables the user to maintain a long-term history of a particular traffic subset. FlowTrackings consist of five graphs of traffic over successive longer time periods: Daily, Weekly, Monthly, Yearly, and Last 3 Years.

[Manage Dashboard](#)

[User's Guide](#)

Select an Active or Archived FlowTracking

Monitoring EOS Science Data Flows

Select a Saved Report

Graph last updated: 04/30/2012 13:47:27 UTC

Graph last updated: 04/30/2012 13:47:27 UTC

Graph last updated: 04/30/2012 13:47:27 UTC

Graph last updated: 04/30/2012 13:47:27 UTC

Select a Saved Report



FlowViewer Main Screen

Links to various tools

User specified links

FlowTrackings

Dashboard (left)

Saved Reports

Dashboard (right)

Dashboard Management

The screenshot displays the FlowViewer main interface. At the top, there are three main sections: "EOS NetOps", "FlowViewer", and "Monitoring EOS Science Data Flows". Below these are navigation tabs for "Select an Active or Archived FlowTracking", "FlowGrapher", "FlowViewer", "FlowTracker", and "Select a Saved Report".

The central "FlowViewer" section is titled "Advancing Network Traffic Situational Awareness" and provides a dynamic web front-end to netflow data collectors and analyzers. It lists three primary tools:

- FlowViewer (FV):** enables the user to create text based reports from filtered netflow data. Several different reporting formats are provided. Each of these reports can be sorted by column heading.
- FlowGrapher (FG):** enables the user to graph the bandwidth used by a filtered subset of netflow data during a specified time period. Resulting reports include the graph and a textual listing of the largest flows.
- FlowTracker (FT):** enables the user to maintain a long-term history of a particular traffic subset. FlowTrackings consist of five graphs of traffic over successive longer time periods: Daily, Weekly, Monthly, Yearly, and Last 3 Years.

At the bottom of the central section are links for "Manage Dashboard" and "User's Guide".

On the left side, under "EOS NetOps", there are four line graphs showing traffic metrics for "RNet to SSC ONE: Last 7 days", "LANSER Reports: Last 7 days", "EOS SR from Hervey: Last 7 days", and "SSC (All) to QRS: Last 24 hours".

On the right side, under "Monitoring EOS Science Data Flows", there are four area charts showing "EOS Flow to the Users: Last 7 days", "SOE Incoming: Last 24 Hours", "SOE Distribution: Last 24 Hours", and "Worldview Graph: Last 4 Weeks".



FlowViewer Input Screen

EOS NetOps

Select an Active or Archived FlowTracking

Graph Last Updated: 04/20/2012 13:47:27 UTC
Maximum: 205.26 Mbps
95thPct: 201.17 Mbps
Average: 258.88 Mbps
Minimum: 9.88 Mbps

Graph Last Updated: 04/20/2012 13:47:27 UTC
Maximum: 584.42 Mbps
95thPct: 636.82 Mbps
Average: 425.17 Mbps
Minimum: 324.17 Mbps

Graph Last Updated: 04/20/2012 13:47:27 UTC
Maximum: 21.62 Mbps
95thPct: 13.82 Mbps
Average: 4.80 Mbps
Minimum: 8.80 Mbps

Graph Last Updated: 04/20/2012 13:47:27 UTC
Maximum: 301.75 Mbps
95thPct: 97.25 Mbps
Average: 14.50 Mbps
Minimum: 8.80 Mbps

FlowViewer

Powered by flow-tools and SILK

FlowGrapher | **FlowViewer** | FlowTracker

Monitoring EOS Science Data Flows

Select a Saved Report

Graph Last Updated: 04/20/2012 13:47:27 UTC

Graph Last Updated: 04/20/2012 13:47:27 UTC

Graph Last Updated: 04/20/2012 13:47:27 UTC

Graph Last Updated: 04/20/2012 13:47:27 UTC

Create a FlowViewer Report

Saved Filters:

Select Saved Filter

Netflow Source:

Test_6589

Select Exporter

Start Date	Start Time	End Date	End Time
4/20/2012	12:00:00	4/20/2012	13:00:00

Source IP Addresses:
192.168.100.0/24, 192.168.200.0/24, -192.168.200.128/28

Source Port	Source AS	Source MT	Source IP Name
			Interface Names

Destination IP Addresses:

Dest Port	Dest AS	Dest MT	Dest IP Name
			Interface Names

TDS Field	TCP Flags	Protocol	NextHop IPx
	DDAC		

Reporting Parameters

Statistics Reports: Source/Destination IP

Printed Reports: Select Print Report

Include Flow If: Any Part in Specified Time Span

Pie Charts: Name

Resolve Addresses: DNS Names

Cutoff Lines: 100

Cutoff Octets:

Sampling Interval:

Octet Units: Use Units

Sort Field: Octets

Generate Textual Report

Reset Form Values

Select an Active or Archived FlowTracking

FlowGrapher | **FlowViewer** | FlowTracker

Select a Saved Report



FlowViewer Input Screen - 1

Setting up a FlowViewer Report

Create a FlowViewer Report

Saved Filters:

Netflow Source:

Report time frame

Start Date	Start Time	End Date	End Time
<input type="text" value="10/24/2012"/>	<input type="text" value="16:00:00"/>	<input type="text" value="10/24/2012"/>	<input type="text" value="17:00:00"/>

Source information

Source IP Addresses:

Source Port: Source AS: Source I/F: Source IF Name:

Destination information

Destination IP Addresses:

Dest Port: Dest AS: Dest I/F:

TOS Field: TCP Flags: Protocol:

Interface Names

- Interface Names
- Include ...
- 0 Interface 0
- 2 ESDIS
- 3 Doors
- 90 Interface 90
- Exclude ...
- 0 Interface 0
- 2 ESDIS
- 3 Doors
- 90 Interface 90

Named interfaces

Report type

Reporting Parameters

Statistics Reports: Printed Reports:

Report output format

Include Flow If: Cutoff Lines: Cutoff Octets: Sampling Multi:

Pie Charts: Resolve Addresses: Octet Units: Sort Field:



FlowViewer Input Screen - 2

Create a FlowViewer Report

Saved Filters: Select Saved Filter (dropdown)

Netflow Source: esro32-core-01a (text input)

Select Exporter (dropdown)

Start Date: 10/24/2012 | Start Time: 16:00:00 | End Date: 10/24/2012 | End Time: 17:00:00

Source IP Addresses (text input)

Source Port (text input) | Source AS (text input) | Source I/F (text input) | Source IF Name (dropdown: Interface Names)

Destination IP Addresses (text input)

Dest Port (text input) | Dest AS (text input) | Dest I/F (text input) | Dest IF Name (dropdown: Interface Names)

TOS Field (text input) | TCP Flags (text input) | Protocol (text input) | NextHop IPs (text input)

Reporting Parameters

Statistics Reports: Source/Destination IP (dropdown menu open)

Select Statistics Report (dropdown menu open):

- Summary
- UDP/TCP Source Port
- UDP/TCP Destination Port
- UDP/TCP Port
- Destination IP
- Source IP
- Source/Destination IP
- Source or Destination IP
- IP Protocol
- Input Interface
- Output Interface
- Input/Output Interface
- Source AS
- Destination AS
- Source/Destination AS
- IP ToS
- Source Prefix
- Destination Prefix

Printed Reports: Select Print Report (dropdown)

Cutoff Lines: 100 (text input) | Cutoff Octets (text input) | Sampling Multi (text input)

Addresses (dropdown) | Octet Units: Use Units (dropdown) | Sort Field: Octets (dropdown)

Reset Form Values (button)

FlowViewer (button) | FlowTracker (button)

Reuse saved filter

Select from different devices

Autonomous systems (flow-tools only)

Report types

Create a FlowViewer Report

Saved Filters Select Saved Filter		Netflow Source Ames_V9_3 Select Exporter		
Start Date 10/24/2012	Start Time 17:00:00	End Date 10/24/2012	End Time 18:00:00	
Source IP Addresses 2001:0D00::/24; 2001:0DA0::/28				
Source Port 80,8080,443	Source AS	Source I/F	Source IF Name Interface Names	
Destination IP Addresses -2002::/16				
Dest Port	Dest AS	Dest I/F	Dest IF Name Interface Names	
TOS Field	TCP Flags 0x000A/0x00AA	Protocol	NextHop IPs	
Reporting Parameters				
Statistics Reports Source/Destination IP	Printed Reports Select Print Report		Sampling Multi	
Include Flow If. Any Part in Specified Time Span	Flow Times AS Numbers 132 Columns 1 Line with Tags AS Aggregation Protocol Port Aggregation Source Prefix Aggregation Destination Prefix Aggregation Prefix Aggregation Source Prefix Aggregation v6 Destination Prefix Aggregation v6 Prefix Aggregation v6 Full Catalyst		Sort Field Objects	
Pie Charts None	Resolve Address DNS Names			
SILK Sources				
all	in	out	inweb	outweb
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Generate Textual Report Reset Form Values

Excluding within a network

Multiple entries

Excluding
(works on all fields)

TCP Flags

When using SILK devices

Sampling multiplier

Additional reports



FlowViewer Report

Can switch to other tools with filtering criteria preserved

EOS NetOps **FlowViewer** Monitoring EOS Science Data Flows
 Powered by flow-tools and SILK

Select an Active or Archived FlowTracking Select a Saved Report

FlowViewer Report from Router_IPv6

Report: Prefix Aggregation v6
 Start Time: 4/30/2012 15:00:00 UTC
 Device Name: Router_IPv6
 Source IPs: /48
 Source Ports:
 Source I/Fs: 1, 4, 5, 6
 Source AS:
 TOS Field:
 Include If: Any Part in Specified Time Span
 Cutoff Lines: 100
 SILK Sources: all

Sort Field: 1
 End Time: 4/30/2012 17:00:00 UTC
 Exporter:
 Destination IPs: /56
 Destination Ports:
 Destination I/Fs:
 Destination AS:
 TCP Flags:
 Protocols:
 Cutoff Octets:

Source Aggregate	Dest Aggregate	Flows	Octets	Packets
200b:48::/48	200b:d70:9700::/56	4	372	4
200b:d70:9700::/48	200b:48::/56	4	770	4
200b:d70:9700::/48	200b:470::/56	4	629	4
200b:470::/48	200b:d70:9700::/56	3	277	3
200b:470::/48	200b:d70:9700:900::/56	3	279	3
2620:0:cc9::/48	200b:d70:9700:900::/56	2	164	2
200b:d70:9700::/48	200b:470:0:100::/56	2	315	2
20a0:1560:5::/48	200b:d70:9700:900::/56	1	102	1
2801:82::/48	200b:d70:9700:900::/56	1	93	1
2800:68:c::/48	200b:d70:9700:900::/56	1	93	1
2610:148:1802::/48	200b:d70:9700::/56	1	93	1
2308:b000:601::/48	200b:d70:9700::/56	1	93	1
2308:b000:601::/48	200b:d70:9700:900::/56	1	93	1
200b:8a0:2106::/48	200b:d70:9700:900::/56	1	93	1
200b:7e8:400::/48	200b:d70:9700:900::/56	1	103	1
200b:d70:9700::/48	20a0:1560:5::/56	1	167	1
200b:d70:9700::/48	2308:b000:601::/56	1	146	1
200b:d70:9700::/48	200b:8a0:2106::/56	1	146	1
200b:1890:1f::/48	200b:d70:9700:900::/56	1	104	1

Select an Active or Archived FlowTracking Select a Saved Report

Aggregation filtering

Sortable by column

Save the filter

Save the report



FlowGrapher Input Screen

Setting up a FlowGrapher Report

Create a FlowGrapher Report

Same filtering criteria

Resolved host names or IP addresses

How to determine statistics (Max, 95th, Avg, Min)

Number of longest flows to list in detail

Time "bucket" size for accumulating bits / period

Save Filters
 Select Saved Filter:

Netflow Source
 test-flow1 Select Exporter:

Start Date: 10/24/2012 Start Time: 17:00:00 End Date: 10/24/2012 End Time: 18:00:00

Source IP Addresses
 172.16.100.64/26

Source Port: Source AS: Source I/F: Source IF Name:

Destination IP Addresses

Dest Port: 514 Dest AS: Dest I/F: 16 Dest IF Name:

TOS Field: TCP Flags: Protocol: NextHop IPs:

Graphing Parameters

Include Flow If: Any Part in Specified Time Span Graph Type: Bits/second Statistics From: Nonzero Values

Resolve Addresses: DNS Names Graph Width: 1 Bucket Size: 2 Sampling Multi: Detail Lines: 200



FlowGrapher Report

EOS NetOps **FlowViewer** Monitoring EOS Science Data Flows
 Powered by flow-tools and SILK

Select an Active or Archived FlowTracking Select a Saved Report

FlowGrapher Report from router-main-01a

Report: FlowGraph Bits/sec
 Start Time: 4/24/2012 6:00:00 UTC
 Device Name: router-main-01a
 Source IPs: seven77.highup.argl.com
 Source Ports:
 Source I/Fs:
 Source AS:
 TOS Field:
 Include If: Any Part in Specified Time Span
 Detail Lines: 200

Bucket Size: 5 sec
 End Time: 4/24/2012 14:00:00 UTC
 Exporter:
 Destination IPs:
 Destination Ports:
 Destination I/Fs:
 Destination AS:
 TCP Flags:
 Protocols:
 Graph Width: 1

Flow data from esro32-core-01a

Bits/Second

Time: UTC

Maximum : 657,387,082
 95th Pct.: 596,828,236
 Average : 464,004,329
 Minimum : 206,273,992

Start	End	Len	Source Host	S Port	Destination Host	D Port	Total Bytes	Mbps
05:34:34	06:06:36	1922.7	seven77.highup.argl.com	55565	192.168.84.128	7326	236,103,048	0.980
05:35:09	06:02:09	1620.7	seven77.highup.argl.com	59185	192.168.84.201	9514	229,663,483	1.130
05:37:14	06:07:36	1822.0	seven77.highup.argl.com	57480	192.168.84.201	9603	259,650,793	1.140
05:44:06	06:16:13	1927.1	seven77.highup.argl.com	55622	219.239.44.225	41191	327,014,700	1.360
05:47:57	06:20:05	1927.4	seven77.highup.argl.com	65461	amc-09-fedora11.ncmcrs.utas.edu.au	36882	317,091,740	1.320
05:52:35	06:19:31	1616.9	seven77.highup.argl.com	55682	192.168.84.201	1146	233,493,593	1.160
05:56:43	06:00:46	242.6	seven77.highup.argl.com	57096	cloudsb-blue.larc.argl.com	14721	863,054,633	28.460

Select an Active or Archived FlowTracking Select a Saved Report

Review of input filtering criteria

Graph of Mbps over specified time period

Calculated statistics

Sortable Columns

Largest flows (e.g., top 200)

Save Filter

Save Report

Mbps per flow (calculated)



FlowTracker Input Screen

Create a FlowTracking

Creating a FlowTracking

Option to start a FlowTracking in the past

Same filtering criteria

Individual or Group FlowTrackings

Email alerting

Alert thresholds

Alert frequency choices

Save Filters

Select Saved Filter Netflow Source Select Exporter

Start Date Start Time (Adjust this only if Recreating a FlowTracking)

Source IP Addresses

Source Port Source AS Source I/F Source IF Name

Destination IP Addresses

Dest Port Dest AS Dest I/F Dest IF Name

TOS Field TCP Flags Protocol NextHop IPs

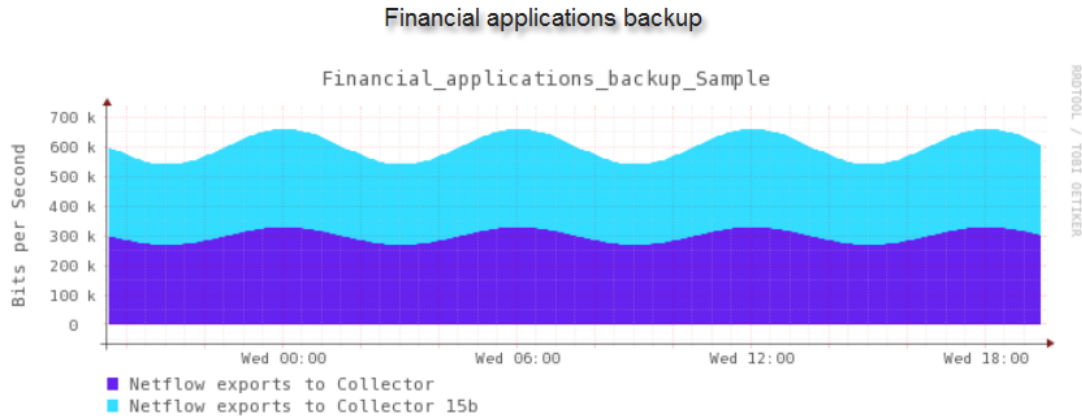
Tracking Parameters

Tracking Label Tracking Type Sampling Multi

Alert Destination (email address) Alert Frequency Alert Threshold

General Comment Alert Frequency choices:

'Groups' stack Individual FlowTrackings →



Select an existing Tracking to be a component of this Group:

Select Individual FlowTracking Group components →

Select a Component:

Place this Component:

Select a Color:

← Can have components above and below X-axis

Add Component

Reset Values

This group is composed of these components:

Adjust Group components →

Netflow exports to Collector 15b	Above 02	auto mixed2	New Color: <input type="text" value="auto mixed2"/>	Move: <input type="text" value="Leave Alone"/>
Netflow exports to Collector	Above 01	auto mixed1	New Color: <input type="text" value="auto mixed1"/>	Move: <input type="text" value="Leave Alone"/>

Adjust the Group

Reset Values

EOS NetOps

FlowViewer
Powered by flow-tools and SILK

Monitoring EOS Science Data Flows

Select an Active or Archived FlowTracking

FlowViewer

FlowTracker

FlowGrapher

Select a Saved Report

FRMR LR from MXG

Device Name: router-core-777
Source IPs: 192.168.243.128/25

Source Ports:
Source IPs:
Source AS:

Exporter:
Destination IPs: -192.168.100.0/16, -192.168.0.0/14, -172.16.10.0/16,
-192.168.0.0/16, -192.1680.0/16, -10.79.0.0/15, -10.119.0.0/16,
-192.168.0.0/16, -10.114.0.0/16

Destination Ports:
Destination IPs:
Destination AS:

FRMR LR from MXG: Last 24 Hours

Bits per Second

1.8 M
1.6 M
1.4 M
1.2 M
1.0 M
0.8 M
0.6 M
0.4 M
0.2 M
0.0

Thu 00:00 Thu 06:00 Thu 12:00 Thu 18:00

Data collected over 5 minute periods: Graph Last Updated: 08/30/2012 16:10:17 UTC

Maximum	1.56 Mbps
95thPct	0.85 Mbps
Average	0.45 Mbps
Minimum	0.09 Mbps

[List Values]

FRMR LR from MXG: Last 7 Days

Second

1.8 M
1.6 M
1.4 M
1.2 M
1.0 M
0.8 M
0.6 M
0.4 M
0.2 M
0.0

Select an Active or Archived FlowTracking

Save Filter

FlowTracker

Save Report

Select a Saved Report

FlowTracking filtering criteria

Statistics kept for graph time period

List individual values

Familiar 'MRTG' graph set

Save Report



EOS NetOps **FlowViewer** Powered by flow-tools and SILK Monitoring EOS Science Data Flows

Select an Active or Archived FlowTracking Select a Saved Report

Can quickly link to either FlowViewer or FlowGrapher (with filter preserved) for more detailed analysis

TEMP IR from MYG: Last 12 Months

Bits per Second

Data averaged over 24 hour periods Graph Last Updated: 08/30/2012 05:30:17 UTC

Maximum	494.81 Mbps
95thPct	311.39 Mbps
Average	155.47 Mbps
Minimum	0.00 Mbps

[List Values]

Scroll down for longer term MRTG-like graphs

TEMP IR from MYG: Last Three Years

Bits per Second

Data averaged over 24 hour periods Graph Last Updated: 08/29/2012 11:50:16 UTC

Maximum	450.77 Mbps
95thPct	250.33 Mbps
Average	146.16 Mbps
Minimum	0.00 Mbps

[List Values]

08/17/2011 18:40:00: Moved to marc-32-15c from 15a

Ability to annotate graphs about significant change events

Select an Active or Archived FlowTracking Select a Saved Report



FlowTracker Report – Group Example

EOS NetOps

FlowViewer Powered by flow-tools and SiLK

Select an Active or Archived FlowTracking

FlowViewer FlowTracker FlowGrapher

Monitoring EOS Science Data Flows

Select a Saved Report

Select a Saved Report

Manage All Saved reports

10/18/2012 14:12:29	FT	EDOS HR from Norway showing 2 days with no 70M peaks
10/15/2012 19:28:55	FT	SD3E to Ocean PEATE Test2 101512
10/15/2012 13:21:13	FT	SD3E to Ocean PEATE Test 101512
10/11/2012 19:05:32	FG	SD3E to Ocean PEATE shows improvement w FW upgrade
10/11/2012 15:08:38	FT	EDOS Open from ASF showing dip
10/10/2012 15:24:18	FG	LADSWEB down for 20 minutes 101012
10/08/2012 14:18:10	FG	EDOS Open typical day - many small 60 second flows
10/05/2012 14:19:05	FG	EDOS Open showing 100 Mbps
10/03/2012 17:41:59	FT	SD3E To UWisc showing switch to chaos from pingest
09/28/2012 14:59:03	FG	129 165 exports FG 092712
09/28/2012 14:57:30	FV	129 165 exports FV 092712
09/26/2012 14:03:11	FT	LADSWEB Exports FW Upgrade 092612
09/25/2012 15:02:35	FG	EOS to NCCS ESRO 092512
09/25/2012 15:02:18	FG	EOS to NCCS ERT0 092512
09/24/2012 13:59:48	FT	LADSWEB - shows FW burst longer than suspect erto netflow export period
09/20/2012 18:00:00	FG	FG Check: ERT0 v ESRO v ESPO

SD3E Testing 071712: Last 4 Weeks

Bits per Second

Data averaged over 2 hour periods

Graph Last Updated: 10/03/2012 17:20:32 UTC

SD3E to Atmos chaos

SD3E to Atmos pingest

SD3E Testing 071712: Last 12 Months

Bits per Second

Data averaged over 24 hour periods

Graph Last Updated: 10/03/2012 08:20:32 UTC

SD3E to Atmos chaos

SD3E to Atmos pingest

Select an Active or Archived FlowTracking

Save Filter FlowTracker Save Report

Select a Saved Report

This FlowTracking documents the delivery of NPP data to the University of Wisconsin. One can see a switch from two (Atmospheric Science) servers to one only, and then all to the other of the pair.

Access to all saved reports

This is an example where you might want to save a FlowTracking



FlowTracker Report – Group Case Study

EOS NetOps FlowViewer Powered by flow-tools and SILK Monitoring EOS Science Data Flows

Select an Active or Archived FlowTracking FlowViewer FlowTracker FlowGrapher Select a Saved Report

EOS to GSFC CNE

EOS to GSFC CNE: Last 24 Hours

Bits per Second

Data collected over 5 minute periods Graph Last Updated: 10/26/2012 20:15:50 UTC

- LADSSCI to GSFC CNE
- LADSWEB to GSFC CNE
- OMI to CNE
- LANCE to GSFC CNE
- ISIPS to GSFC CNE

Each legend item 'hyperlinks' back to the Individual FlowTracking

This example depicts a situation where traffic shaping was invoked to manage limited network resources. This FlowTracking Group helps identify if perhaps there is one 'big player' for which a different network arrangement might mitigate the problem

EOS to GSFC CNE: Last 7 Days

Bits per Second

Data averaged over 30 minute periods Graph Last Updated: 10/26/2012 20:00:50 UTC

- LADSSCI to GSFC CNE
- LADSWEB to GSFC CNE
- OMI to CNE
- LANCE to GSFC CNE

Select an Active or Archived FlowTracking Save Filter FlowTracker Save Report Select a Saved Report

January 11, 2013

21



FlowTracker Management

Pulldown of all FlowTrackings

Listing of all FlowTrackings

EOS NetOps | **FlowViewer** | **FlowTracker** | **FlowGrapher** | **Monitoring EOS Science Data Flows**

Select an Active or Archived Flow Tracking

Manage All FlowTrackings

- Individuals
- ASTER to GSFC After
- Baidu Spider
- Closed EBnet to Open EBnet Primary
- Doors to Stanford Univ.
- EBnet Input
- EBnet Output
- EBnet to AZTI (Spain)
- EBnet to ESA ESTEC (NL)
- EBnet to GSFC CNE
- EBnet to GSFC SEN
- EBnet to I2
- EBnet to ICIMOD (Nepal)
- EBnet to NMSU
- EBnet to NSSTC (GUFC)

SD3 Traffic In

SD3 Traffic Out

SD3E from CLASS

SD3E from CLASS ERT032

SD3E from FTP.CLASS.NOAA.GOV

SD3E from IDPS

SD3E from NSOF

SD3E from RIP Server

SD3E to Atmos chaos

SD3E to Atmos pingest

SD3E to Atmosphere PEATE

SD3E to Ocean PEATE

SD3E to SIGMA

SD3E to SIGMA Space

SD3E to Sounder PEATE

SDS LAND to NICSE

SDS to CLASS

SEN to EBnet

Starlight to EDC from NASA

Starlight to EDC from non-NASA

TSDIS

TSDIS to Internet

Univ of Alaska to GSFC

Unlabeled

Worldview

Worldview All

Worldview Ingest1

Worldview Ingest2

Worldview Map 1

Worldview Map 2

Group Trackings

EBnet Input and Output

EBnet to GSFC Campus

EDC to Starlight

EOS and NCCS

EOS CNE Flows fasadmin

EOS exchange with NOAA

EOS Flows to the Doors

EOS to GSFC CNE

Revise

Rename

Archive

Remove

Select a Saved Report

EOS Flows to the Doors: Last 7 days

SD3E Incoming: Last 24 Hours

SD3E Distribution: Last 24 Hours

EOS to NISN PIP: Last 4 Weeks

Case Studies

Components of an Interface

Satellite data in

Science data out

To service provider

Ability to 'Revise', 'Rename', 'Archive', 'Remove', and 'Restore' FlowTrackings



EOS NetOps

FlowViewer
 Powered by flow-tools and SILK

Monitoring EOS Science Data Flows

Select an Active or Archived FlowTracking ▾
FlowViewer
FlowTracker
FlowGrapher
Select a Saved Report ▾

EDOS HR from Norway: Last 7 Days

Bits per Second

Data averaged over 30 minute periods

Graph Last Updated: 10/26/2012 21:00:50 UTC

Maximum	31.74 Mbps
95thPct	15.54 Mbps
Average	4.48 Mbps
Minimum	0.00 Mbps

■ Peak 5 Minute Period [List Values]

EDOS HR from Norway: Last 4 Weeks

Bits per Second

Data averaged over 2 hour periods

Graph Last Updated: 10/26/2012 20:40:50 UTC

Maximum	18.79 Mbps
95thPct	12.46 Mbps
Average	5.87 Mbps
Minimum	0.93 Mbps

■ Peak 5 Minute Period [List Values]

Select an Active or Archived FlowTracking ▾
Save Filter
FlowTracker
Save Report
Select a Saved Report ▾

Gray line preserves highest 5-minute measurement over the longer term graphs

These graphs help NASA monitor an expensive high-rate circuit between a polar ground station in Norway and the GSFC in Maryland. The circuit is shared with other Federal agencies through the use of MPLS tunnels.

This depression of peak values indicates that there may be an issue with the network or the MPLS tunnel (or the servers, or software or, ...)



EOS NetOps

Select an Active or Archived FlowTracking

FlowViewer

Powered by flow-tools and SiLK

FlowViewer FlowTracker FlowGrapher

Monitoring EOS Science Data Flows

Select a Saved Report

Around the time of last summer's hurricane Isaac, Land, Atmosphere Near-Real-Time Capability for EOS (LANCE-MODIS*) system managers noted a sharp increase in traffic.

The FlowTracker Re-create capability was invoked to create a FlowTracking Group which isolated the new user that had come on line: the National Severe Storms Laboratory.

LANCE by Destination: Last 7 Days

Data averaged over 30 minute periods Graph Last Updated: 09/05/2012 15:30:20 UTC

- LANCE to NAIL NATICE at NOAA
- LANCE to Other
- LANCE to NAT NSSL at NOAA

LANCE by Destination: Last 4 Weeks

Data averaged over 2 hour periods Graph Last Updated: 09/05/2012 14:50:20 UTC

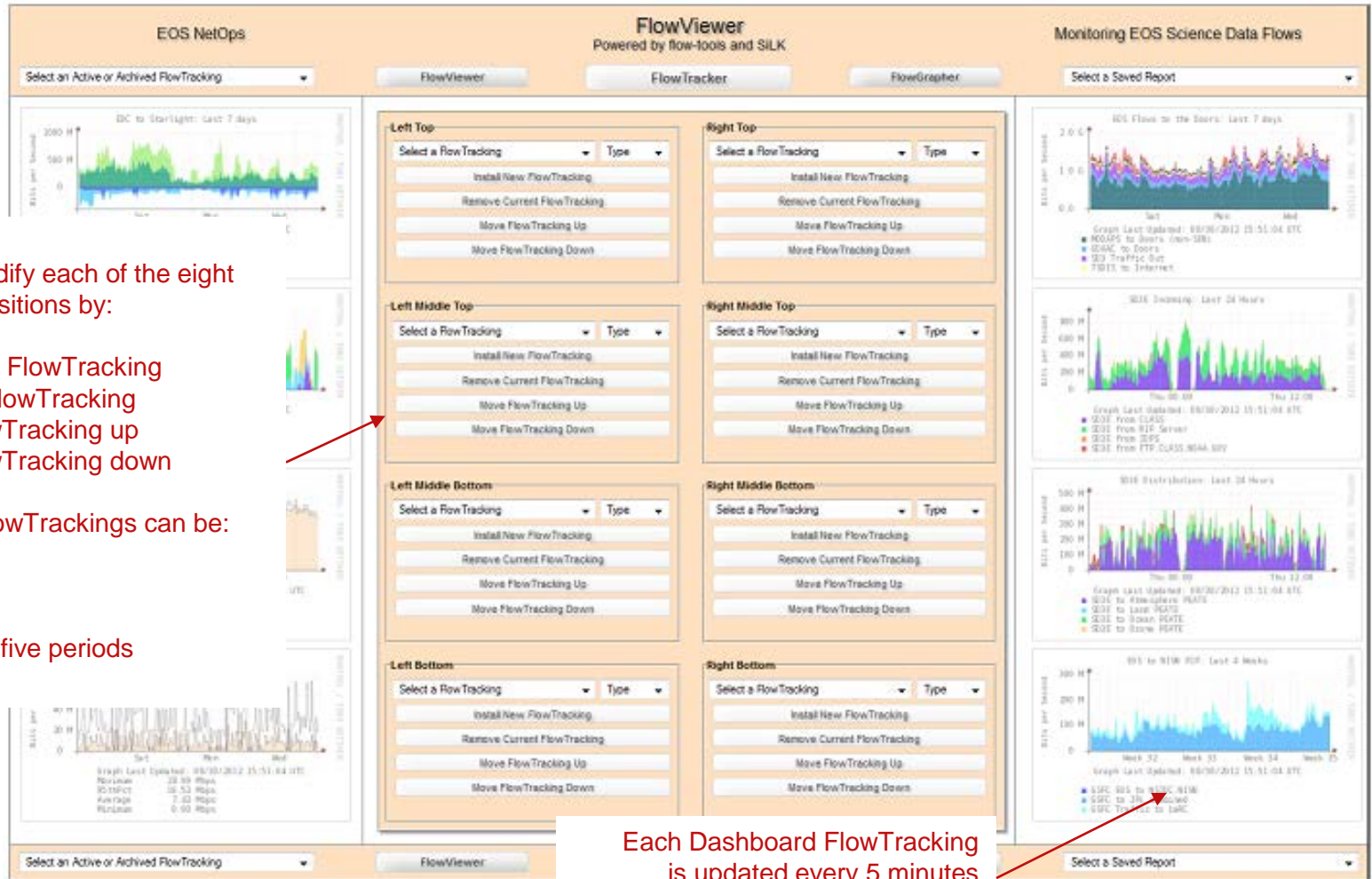
- LANCE to NAIL NATICE at NOAA
- LANCE to Other
- LANCE to NAT NSSL at NOAA

* MODIS - Moderate Resolution Imaging Spectroradiometer

Select an Active or Archived FlowTracking

FlowViewer FlowTracker FlowGrapher

Select a Saved Report



Users can modify each of the eight Dashboard positions by:

- 1) Install new FlowTracking
- 2) Remove FlowTracking
- 3) Move FlowTracking up
- 4) Move FlowTracking down

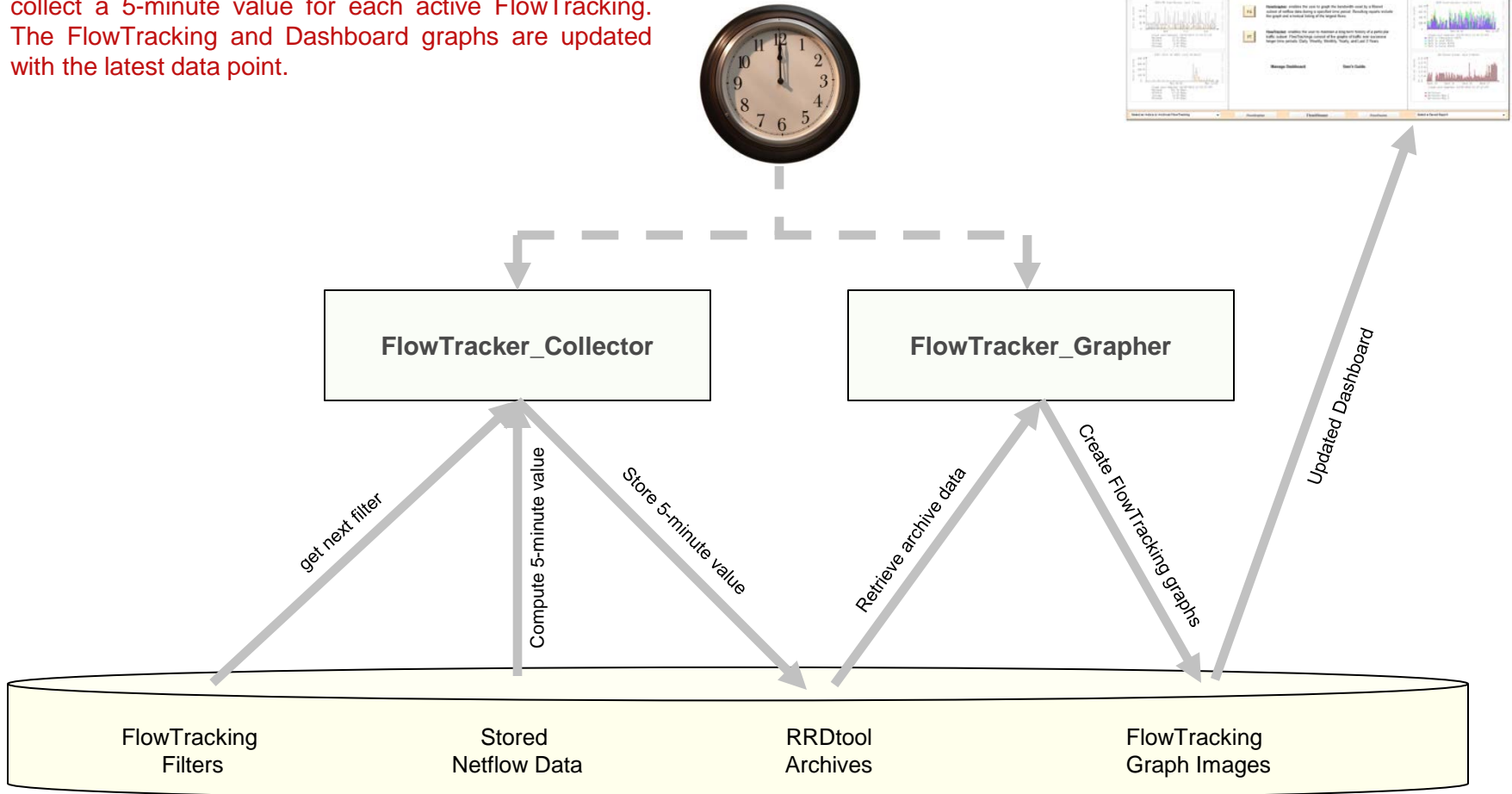
Dashboard FlowTrackings can be:

- 1) Individual
- 2) Group
- 3) Any of the five periods

Each Dashboard FlowTracking is updated every 5 minutes

Each Dashboard graph links back to the original FlowTracking

Upon FlowViewer installation, the FlowTracker_Collector and FlowTracker_Grapher scripts are placed in the Linux background. They will “wake up” every five minutes and collect a 5-minute value for each active FlowTracking. The FlowTracking and Dashboard graphs are updated with the latest data point.



- FlowViewer distribution includes “analyze_netflow_packets” utility
- FlowViewer has supported flow-tools for over five years; but is new to SiLK
- Integration with SiLK may not be optimized as a result
- Would welcome SiLK related improvement suggestions
- At the same time ... some ‘requests’ of SiLK 😊. Please include:
 - IPFIX Information Element (IE) [5]: `ipClassOfService`
 - IPFIX Information Element (IE) [16]: `bgpSourceAsNumber`
 - IPFIX Information Element (IE) [17]: `bgpDestinationAsNumber`
 - IPFIX Information Element (IE) [70]: `mplsLabelStackSection`
 - IPFIX Information Element (IE) [71]: `mplsLabelStackSection2`
 - IPFIX Information Element (IE) [72]: `mplsLabelStackSection3`



Thank You

Joe Loiacono
Network Engineer, CSC
jloiacon@csc.com

<http://earthdata.nasa.gov/esdis>

NASA Official: Kevin Kranacs
Manager, ESDIS Networks

FlowViewer is available from:
<https://sourceforge.net/projects/flowviewer>